IN THE CLAIMS:

Please amend claims 1, 5, 7-13, 15-16, 19-21, and 24-25, and ADD claims 26-28 as follows.

1. (Currently Amended) A method in a communication system wherein a serving controller is configured to support a first security mechanism and at least one other security mechanism, the method comprising:

sending a request for registration from a user equipment to a serving controller via a second controller, said request for registration including information indicative of at least one security mechanism supported by the user equipment;

determining, based on the ~~request~~information, in ~~a~~ the second controller that the user equipment supports a second security mechanism other than a first security mechanism;

removing the information from the request for registration in the second controller, including in the request for registration ~~sending from the second controller to the serving controller~~ an indication that the second security mechanism is used by the user equipment and forwarding the request for registration including said indication to the serving controller; and

sending a challenge in accordance with the second security mechanism from the serving controller to the user equipment.

2. (Original) A method as claimed in claim 1, further comprising:

including a response to the challenge in a message from the user equipment to the serving controller.

3. (Original) A method as claimed in claim 2, further comprising:

using the response for authentication of the message at the serving controller.

4. (Original) A method as claimed in claim 1, further comprising:

providing the second controller comprising a network entity providing proxy call state control functions between the user equipment and the serving controller.

5. (Currently Amended) A method as claimed in claim 1, wherein the ~~step of~~ sending of the request for registration from the user equipment to the serving controller comprises

sending a challenge from the serving controller to the user equipment, sending a response to the challenge from the user equipment, and

registering the user equipment to the serving controller only if a satisfactory response is received from the user equipment, and sending a further challenge to the user equipment after the registration is completed.

6. (Original) A method as claimed in claim 1, further comprising:

obtaining data for sending the challenge from a user information database.

7. (Currently Amended) A method as claimed in claim 1, wherein the ~~step of~~ sending of the challenge comprises sending the challenge comprising an authentication vector.

8. (Currently Amended) A method as claimed in claim 1, further comprising:

providing the first security mechanism comprising a security mechanism in accordance with a ~~Secure Internet Protocol.~~secure internet protocol.

9. (Currently Amended) A method as claimed in claim 1, ~~wherein the~~further comprising:

providing the second security mechanism comprising a security mechanism in accordance with a ~~Hypertext Transfer Digest protocol.~~hypertext transfer digest protocol.

10. (Currently Amended) A method as claimed in claim 1, further comprising:

sending of at least the challenge or a response in a message in accordance with a ~~Session Initiation Protocol.~~session initiation protocol.

11. (Currently Amended) A method as claimed in claim 1, further comprising:

registering the user equipment with a serving controller of an ~~Internet Multimedia Subsystem.~~internet multime

12. (Currently Amended) A method as claimed in claim 2, wherein said information comprises a list of security mechanisms supported by the user equipment further comprising:

including in a security-client header of the request for registration ~~a~~ the list of security mechanisms supported by the user equipment;

concluding at the second controller based on the list that the user equipment supports the second security mechanism instead of the first security mechanism;

removing the security-client header from the request and including into an authorization header of the request ~~an~~ the indication that the second security mechanism is to be used; and

forwarding the request to the serving controller.

13. (Currently Amended) A method as claimed in claim 1, wherein the ~~step of~~ sending of the challenge comprises sending the challenge to the user equipment in an authentication information header of a message.

14. (Original) A method as claimed in claim 3, further comprising:

providing the message comprising a request for a service provided by an application server.

15. (Currently Amended) A communication system comprising:

a serving controller configured to accept registrations of user equipments and to support at least two different security mechanisms; and

~~means for providing~~ a unit configured to receive from a user equipment in a request for registration data indicative of at least one security mechanism that the user equipment supports, to remove said data from the request for registration, to provide the serving controller with information regarding a security mechanism supported by ~~a~~ the user equipment that has requested to be registered to the serving controller, and to forward the request for registration to the serving controller, wherein the serving controller is configured to send a challenge in accordance with a determined security mechanisms to the user equipment and to authenticate a message from the user equipment based on a response to the challenge included in the message.

16. (Currently Amended) A communication system as claimed in claim 15, wherein the providing ~~means for~~unit configured to provide information regarding ~~a supported~~ the security mechanism ~~are~~ is provided in a second controller.

17. (Original) A communication system as claimed in claim 16, wherein the second controller comprises a network entity providing proxy call state control functions between the user equipment and the serving controller.

18. (Original) A communication system as claimed in claim 15, further comprising:

a user information database configured to store data associated with challenges.

19. (Currently Amended) A communication system as claimed in claim 15, wherein the serving controller is configured to support a security mechanism in accordance with a ~~Secure Internet Protocol.~~secure internet protocol.

20. (Currently Amended) A communication system as claimed in claim 15, wherein the serving controller is configured to support a security mechanism in accordance with a ~~Hypertext Transfer Digest protocol.~~hypertext transfer digest protocol.

21. (Currently Amended) A communication system as claimed in claim 15, the communication system comprising an ~~Internet Multimedia Subsystem.~~internet multimedia subsystem.

22. (Original) A communication system as claimed in claim 15, further comprising:

a connection to an application server, wherein a message subjected to authentication by the servicing controller based on the response to the challenge comprises a request for a service provided by the application server.

23. (Original) A communication system as claimed in claim 15, wherein the message subjected to authentication by the servicing controller based on the response to the challenge comprises a request for registration to the serving controller.

24. (Currently Amended) A proxy controller for a communication system, ~~the proxy controller being~~ configured to receive a request for registration from a user equipment for forwarding to a serving controller, said request including data indicative of at least one security mechanism supported by said user equipment, to determine based on said data a security mechanism supported by ~~a~~ the user equipment that has requested ~~for registration~~to be registered to the serving controller, to remove the data from the request for registration in the second controller before forwarding said request to the serving controller, and to signal information to the serving controller regarding the security mechanism supported by the user equipment.

25. (Currently Amended) A communication system comprising:

first sending means for sending a request for registration from a user equipment to a serving controller via a second controller, said request including information indicative of at least one security mechanism supported by the user equipment;

determining means for determining, based on the ~~request~~information, in a second controller that the user equipment supports a second security mechanism other than a first security mechanism;

removing means for removing at said second controller said data;

second sending means for sending from the second controller to the serving controller an indication that the second security mechanism other than the first security mechanism is used by the user equipment; and

third sending means for sending a challenge in accordance with the second security mechanism from the serving controller to the user equipment.

26. (New) A communication system comprising:

serving controller means for accepting registrations of user equipments and to support at least two different security mechanisms; and

means for receiving from a user equipment in a request for registration data indicative of at least one security mechanism that the user equipment supports, removing said data from the request for registration, providing the serving controller with information regarding a security mechanism supported by the user equipment that has requested to be registered to the serving controller, and forwarding the request for registration to the serving controller, wherein the serving controller is configured to send a challenge in accordance with a determined security mechanism to the user equipment

and to authenticate a message from the user equipment based on a response to the challenge included in the message.

27. (New) A proxy controller for a communication system, the proxy controller comprising:

receiving means for receiving a request for registration from a user equipment for forwarding to a serving controller said request including data indicative of at least one security mechanism supported by said user equipment;

determining means for determining, based on said data, a security mechanism supported by the user equipment that has requested to be registered to the serving controller;

removing means for removing the data indicative from the request for registration in the second controller before forwarding said request to the serving controller; and

signalling means for signalling information to the serving controller regarding the security mechanism supported by the user equipment.

28. (New) A communication system comprising:

a first sending unit configured to send a request for registration from a user equipment to a serving controller via a second controller, said request including information indicative of at least one security mechanism supported by the user equipment;

a determining unit configured to determine, based on the information, in a second controller that the user equipment supports a second security mechanism other than a first security mechanism;

a removing unit configured to remove at said second controller said data;

a second sending unit configured to send from the second controller to the serving controller an indication that the second security mechanism other than the first security mechanism is used by the user equipment; and

a third sending unit configured to send a challenge in accordance with the second security mechanism from the serving controller to the user equipment.